June 27, 2022 - CISA Community Bulletin

CISA Releases Election Security Insider Threat Mitigation Guide

CISA released the [Election Infrastructure Insider Threat Mitigation Guide] which offers election stakeholders guidance on understanding and mitigating insider threats. This guide helps stakeholders define insider threats, highlights elections risks, and provides guidance on how to improve insider threat mitigation practices. Additionally, it helps organizations establish insider threat mitigation programs that are both proactive and reactive to potential threats. CISA emphasizes the importance of a positive, supportive organizational culture with four key measures in place:

- Standard operating procedures,
- Access control,
- Zero trust security, and
- Chain of custody.

CISA has also developed an accompanying training and postcard on insider threat mitigation for election stakeholders that is available upon request.

Visit www.cisa.gov/election-security-library for additional resources.

Learn More Here

Alerts & Announcements

Fiscal Year 2022 SAFECOM Guidance on Emergency Communications Grants Released

CISA published the fiscal year 2022 *SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance)* in partnership with SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC).

The SAFECOM Guidance is updated every year with partners' input to assist organizations who are planning or applying for federal emergency communications funding. The guidance provides information on what activities are eligible, the technical standards, and other terms and conditions common to most federal emergency communications grants.

For this year's release, CISA consulted federal partners and the Emergency Communications Preparedness Center to ensure the guidance's emergency communications policies are coordinated and consistent across the federal government. It also reflects the current public health and cybersecurity landscapes, investment priorities, technical standards, and available supporting materials for implementing emergency communications projects. Key changes to the guidance include information on the Infrastructure Investment and Jobs Act, American Rescue Plan Act, and Project 25 compliance.

To read the most recent SAFECOM Guidance visit here.

Learn More Here

THE NECP
National Emergency Communications Plan
NECP SPOTLIGHT
Implementing UAS Programs to Support Emergency Operations
For more information, visit: cisa.gov/necp
CISA

New NECP Spotlight: Aligning Emergency Communications in Preparation for the Super Bowl

The Super Bowl was labeled as a National Special Security Event. This allows federal, state, local, and private sector agencies to work together to ensure emergency communications every year. These emergency response agencies collaborate to plan and train for security operations at the Super Bowl each year. The planning involves development of risk management strategies to ensure emergency communications interoperability on Super Bowl night.

The National Emergency Communications Plan (NECP) Spotlight: Aligning Emergency Communications in Preparation for the Super Bowl examines how public safety agencies worked together before, during, and after the Super Bowl to ensure reliable and interoperable communications throughout the event.

The NECP emphasizes the importance of emergency planning by means of training and exercises, information sharing, and continuity of communications. Visit www.cisa.gov/necp to read the full spotlight and stay up to date on the latest NECP Spotlights.

Learn More Here

NECP Webinar: How is 5G Impacting Emergency Communications?

Join CISA for the *How is 5G Impacting Emergency Communications* webinar on June 29. During this webinar, learn about the CISA 5G Strategy, the current 5G deployment status, and how to use the National Emergency Communications Plan to address emerging technology challenges.

Date: June 29, 2022

Time: 1:00 p.m. - 2:00 p.m. ET

Learn More Here

CISA's Office for Bombing Prevention Releases Mass Bomb Threat Awareness Products

CISA recently has seen an uptick in strategic mass bomb threat campaigns against critical infrastructure. The threat actors are targeting election polling locations, higher education institutions, medical facilities, and faith-based organizations. Just this year, a wave of bomb threats targeted Historically Black Colleges and Universities and Jewish Community Centers.

To prepare for and respond to mass bomb threats, CISA's Office for Bombing Prevention (OBP) developed a postcard and bulletin that offer risk management guidelines and resources to protect personnel and infrastructure. OBP's new Mass Bomb Threat Postcard outlines the different bomb threat levels and appropriate actions to take. The postcard also provides critical information on the indicators of a bomb threat and its potential impact on an operational and psychological level.

OBP also recently released a TRIPWire Awareness Bulletin for Responding to Mass Bomb Threat Campaigns. The bulletin provides resources on how to response to bomb threat campaigns and information on previous mass bomb threat campaigns. These resources include virtual and in-person trainings, checklists, educational videos, and more.

For information about these and other resources to help stakeholders react to bomb threats or suspicious items, see OBP's What to Do: Bomb Threat Resources page.

Learn More Here

Quarterly ChemLock Trainings

CISA's ChemLock program provides the ChemLock: Introduction to Chemical Security training course quarterly on a first-come, first-serve basis. This course provides an introduction to identifying, assessing, evaluating, and mitigating chemical security risks. This easy-to-understand overview identifies key components and best practices of chemical security awareness and planning to help kick start chemical security discussions at your facility.

This course runs 1 to 2 hours and is appropriate for all personnel regardless of their level of involvement with dangerous chemicals.

- Register for July 13, 2022 – 9-11 am ET
- Register for October 13, 2022 – 11 am-1 pm ET
- Register for January 11, 2023 – 3-5 pm ET
- Register for April 12, 2023 – 1-3 pm ET

For more information or to request a specific training for your facility, please visit the ChemLock Training webpage.

Learn More Here

15th Anniversary for Chemical Facility Anti-Terrorism Standards (CFATS) Program

The Chemical Facility Anti-Terrorism Standards (CFATS) program is celebrating 15 years of working with high-risk facilities to enhance the security of dangerous chemicals. As part of this celebration, CISA is releasing a blogs series that tell the story of CFATS, from the very beginning to the continued efforts during the COVID pandemic. The first blog highlighted the environment that made chemical security a priority and how the CFATS program began. Learn more on the CFATS 15th Anniversary webpage.

CISA Announces Multifactor Authentication Campaign

On June 6, CISA announced a collaborative effort with industry to dramatically increase adoption of multi-factor authentication (MFA) and ensure widespread understanding of why it is one of the strongest tools to prevent cyber intrusions.

After launching at the 2022 RSA Conference, CISA is embarking on a campaign to encourage widespread awareness and understanding of the benefits of MFA, to ensure that every American knows the simple steps they can take to keep themselves safe online, and to urge technology companies to make MFA available as a default option.

CISA's *More Than a Password* campaign includes a newly launched webpage with resources, how-to guides, and social media content throughout the month of June. Multi-Factor Authentication | CISA

Learn More Here

CISA Releases Sector Spotlight: Cyber-Physical Security Considerations for the Electricity Sub-Sector

CISA published the *Sector Spotlight: Cyber-Physical Security Considerations for the Electricity Sub-Sector.*

CISA and the Department of Energy (DOE) developed the sector spotlight to help small and mid-sized municipalities, utility owner operators, and the broader critical infrastructure community better understand the cyber and physical risks associated with the electricity sub-sector. This spotlight seeks to highlight the various threat vectors to the sub-sector, provide recommendations and methodologies for maintaining resiliency, and connect stakeholders to the suite of tools and resources provided by CISA and DOE. Additionally, this spotlight provides a simplified visual representation of the electricity generation, transmission, distribution, and consumption components of the grid.

This resource is an example of CISA's commitment to leading the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. For more information and to access this resource, visit: https://www.cisa.gov/publication/convergence-security-guide-electricity-sub-sector.

Social Media

Help CISA spread the word about upcoming events and new resources by sharing the following posts via your social media channels. Thank you for your support!

- Don't forget to check out the new infrastructure dependency primer. Find out more here: https://www.cisa.gov/idp.
- Want to learn more about recent cybersecurity alerts? Check out @CISAgov's National Cyber Awareness System: https://www.cisa.gov/uscert/ncas/alerts.
- @CISAgov encourages stakeholders to remain vigilant when accessing information online. For the latest internet protocol guidance, click here: https://www.cisa.gov/tic.

To access past editions of the CISA Community Bulletin newsletter, please visit the CISA Community Bulletin archive.